International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

SecuIIoT: Hyper-Tuned Adaptive Learning for Cognitive Detection of Industrial IoT (IIoT) Cyber Threats

S Gouri Kiran Kumar[1], Dr Raavi Satya Prasad[2]

Department of Information Technology, College of Computing and Information Sciences, University of Technology and Applied Sciences, Muscat, Oman
kiran43427@gmail.com, gouri.kiran@utas.edu.om
Professor and Dean R & D, Department of Computer Science & Engineering, Dhanekula Institute of Engineering & Technology, Ganguru, Vijayawada, A.P., India, deanresearch@diet.ac.in; orcid: 0009-0007-1894-2417.

Abstract:

Industrial automation has been advanced by the explosive growth of the Industrial Internet of Things (IIoT), but also has become markedly more susceptible to cyber attacks. This paper introduces intelligent and adaptive security framework called SecuIIoT which discovered the attacks in IIoT. SecuIIoT uses Hyper-tuned Ensemble Learning models that include algorithms, like ResNet50 as pre-trained model, XGBoost for feature extraction and Logistic Regression (LR) for final classification, with automatic hyper parameter optimization in order to increase the detection accuracy and reduce the rate of false positive (FP). Utilizing a cognitive approach to learning, the cognitive learning system dynamically learns from new threat patterns and changing network behaviors. The model is trained and tested from China IIoT cyber-attacks benchmark datasets and enables to achieve better accuracy of 98.78%, precision of 98.78%, recall of 97.34%, and F1-score of 98.41% compare to the traditional classifiers. The proposed method not only advances the real-time threat recognition, but also empowers the scalability and the robustness of the model, thus could be well tailored to work in large-scale industrial infrastructures. SecuIIoT represents a significant step forward in proactive IIoT security through the use of adaptive intelligence with tuned learning strategy.

Keywords: XGBoost, Logistic Regression (LR), ResNet50, Industrial Internet of Things (IIoT).

1. Introduction

With the growing dependence on digital infrastructure and the rapidly expanding interconnected complexity of systems, the threat of cyber attacks has been elevated to an unprecedented level in such application domains as industrial systems, healthcare, finance, and smart cities. With the advancement and evolution of cyberspace attacks in a more and more sophisticated manner, traditional security technologies like firewalls and rule-based intrusion detection systems (IDS), as well as signature-based antiviruses, are by far not enough to catch and protect from modern, adaptive and polymorphic threads: Zero Day exploits, Advanced Persistent Threats (APTs) and polymorphic malware. Cyber attack

detection is recognizing unknown and/or unauthorized activities on a computer system, a network environment, or existing applications. Timely detection prevents data compromises, service outages, and financial and reputational injury. Advances in artificial intelligence (AI) and machine learning (ML) have made it possible to build more powerful, intelligent detection systems that can learn and adapt from vast amounts of security-relevant data to identify subtle and intricate patterns of abnormal behavior.

Ensemble learning models, e.g., by using a combination of multiple base learners to enhance generalization and accuracy, have demonstrated their success in cyber threat detection. After hyper-tuning and adaptive training, such models perform better than the single model-based method because the detection sensitivity increases with the decrease in false positives. Additionally, by combining DL techniques for insights and implementing pre-trained models, the model can identify known and novel threats in live traffic. The attack surface has increased dramatically since the development of the IIoT, which connects internet-enabled devices with massive sensor networks and industrial controls. Therefore, creating intelligent and adaptable cyber detection systems specifically for IIoT environments has become a key area of research and development effort. This paper aims to investigate and design a hyper-tuned adaptive ensemble learning scheme for detecting cyber attacks intelligently in IIoT and other mission-critical environments. With the benefit of different ML paradigms and tuning for high-throughput threat detection, we aim to deliver a scalable, online, and proactive cyber-defense system.

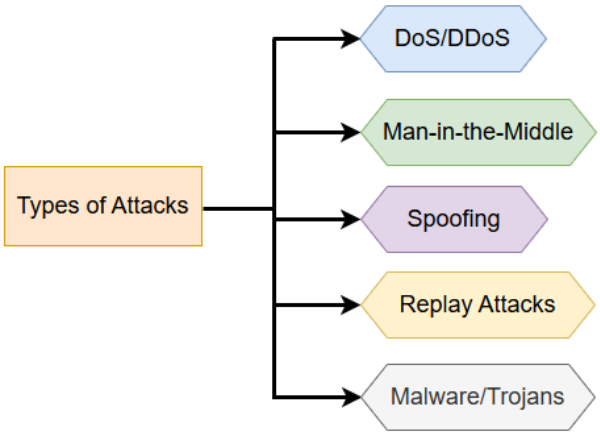

Figure 1: Different Types of Cyber Attacks

2. Literature Survey

Ponnapalli et al. [11] introduced Blockchain technique integrated with cloud computing, SSD2P to overcome the problems of data tampering and unauthorized access and delivery delay. The system employs a decentralized ledger based on blockchain to guarantee transparency, immutability, and traceability of the data transactions. Policies for sharing data are automatically enforced using smart contracts, and an energy-efficient consensus mechanism is provided for fast verification. Also, to preserve the data propagation speed, a compact encryption process is implemented without losing data privacy. The performance of which is calculated using DDL of 27.4%,and DIS of 99.89%. Ponnapalli et al. [12] presented a hybrid learning approach that aggregates the power of CNN in spatial-side and LSTM networks in temporal-side. Ensemble-technique and feature selection by mutual information are further applied to refine the hybrid model for better detection accuracy. Experiments were performed

with benchmark data sets such as UNSW-NB15 yielding the (Acc) of 97.4%, (Pre) of 96.8%, (Recall) of 97.1%, (F1S) of 96.9% and FPR of 1.2%, for the CICIDS2017 data set the (Acc) of 98.1%, (Pre) of 97.6%, (Recall) of 98.0%, (F1S) of 97.8% and FPR 0.9%, covering a broad category of cloud-specific attack vectors.

Dornala et al. [13] presented a new quantum-inspired fault-tolerant load balancing mechanism that was based on quantum principles (i.e., quantum superposition and entanglement), for real-time task-allocation to cloud resources. Our framework presents a hybrid quantum-classical algorithm, which combines Grover's search and quantum parallelism to form the algorithm, aimed at finding the least-loaded and most-available virtual machines (VMs). In order to increase fault-tolerance, the system is using quantum error correction, as well as a redundancy-aware load allocation. The model monitors fault and does reassign in a dynamic way and work with quantum- aided decision-making. Overall, the performance of proposed approach achieved the ATCT (ms) of 121, System Throughput (tasks/sec) of 141, and FRR (%) of 96.74%. Dornala et al. [14] introduced an ensemble learning approach for resource allocation which utilizes the Optimized PSO for dynamic allocation of cloud resources. Although the traditional PSO techniques have been accepted and proven effective, it often falls into the shortcomings of prematurity convergence and sub-optimal load distribution in high dimensional search space. In order to deal with these problems, we come up with an ensemble learning process, which integrates the predictability of multiple heuristic models, as well as an improved PSO variant tuned by adaptive inertia weight and velocity constraints. The PSO can learn from the historical model's data and make allocation decision more accurately and reasonably, to use historical workloads pattern and performance metrices as guidance to PSO. The outcomes reveal that the developed ensemble-led optimized PSO is much better than conventional algorithms. It is 13.9% better in terms of makespan, and 14.3% higher in terms of resource utilization compared to the regular PSO.

Kamma Prasanth [15] discussed development and evolution of an AI based DSS that exploits machine and deep learning algorithms in order to improve the clinical outcome in different medical areas, like cardiology, oncology, and critical care. The proposition uses predictive algorithms, pattern recognition and natural language processing to understand structured and unstructured data. For binary diseases classification, the DSS attained a mean sensitivity of 92.7% on 5, ranging from 15%–20% more thank the state-of-the-art rule-based systems. AL-Hawawreh et al. [16] introduced a DL-based system for accurate detection and categorization of malicious behaviors in IIoT settings. With the help of LSTM and CNN the system extracts temporal and spatial characteristics of IIoT traffic data. The proposed model is trained and tested on two normal and attack scenarios in a well-known IIoT cybersecurity dataset. Results of the deep learning-based IDS demonstrate a detection (Acc) of 98.34%, (Pre) of 97.98%, and Recall of 97.45%, whereas the FPR is 1.06, and thus the IDS outperforms conventional machine learning detectors.

Sitnikova et al. [17] presented the results on theperformance of hands-on exercises in SCADA cybersecurity education. The students not only practice with simulation-based labs and virtual SCADA environments but also engage in real-time attack-defense scenarios. Thus, they are exposed to situations that improve their hands-on conceptualization of SCADA system security alongside incident response. The research output metrics include the average performance (Acc) of the students, which stood at 92%. Abdel-Basset et al. [18]describes the development of Deep-IFS, a novel Deep Learning-based IDS that

specifically designed to operate in the simulated IIoT network with fog computing architecture. The model operates as a semi-streaming system by using a sliding window to analyze traffic patterns accurately and send threat detection decisions, thus reducing latency. Deep-IFS operates by accelerated quasi-static pattern matching. To counteract the dataset's imbalanced distribution during training, the training dataset incorporates the SMOTE technique. Furthermore, the two benchmark datasets, TON_IoT and NSL-KDD, are also used in training the model. Lastly, the model is efficient in terms of energy and memory. Notably, by optimizing for energy efficiency, the model is suitable to train in the simulated fog nodes. The model's average performance based on the (Acc) stood at above 98 %, surpassing traditional ML techniques.

Pre-Trained Model: ResNet50

The rapid proliferation of connected devices and the IIoT has dramatically increased digital infrastructures' cyber threat surface area. Therefore, quickly and accurately detecting threats still poses a significant challenge in cybersecurity. However, deep learning models, especially CNNs, have demonstrated the potential to automate threat detection through pattern recognition of network traffic datasets. An excellent example of deep CNNs is ResNet50, a 50-layered deep CNN capable of residual learning, making it optimal for feature extraction and classification. Although ResNet50 was initially designed for image classification, it can be fine-tuned for cybersecurity datasets by reimagining the network behavior patterns as image-like representations. For example, the behavior of a network traffic flow can generate image features, byte-level image representation, or deviate the time-series signal into image-like representations. Notably, the transfer learning approach helps to fine-tune the model using the pre-trained weights of ResNet50. The transfer learning approach is critical since it shortens the training duration and improves generalization and accuracy. In the case of cyber threat detection, ResNet50 acts as an anomaly detector and intrusion detection sensor by learning from labeled datasets containing a variety of cyber-attacks, including DoS, BDoS, botnets, and infiltration threats. The approach becomes essential for advanced and intelligent threat detection, and it would strengthen the security preparedness of enterprising and industrial systems.

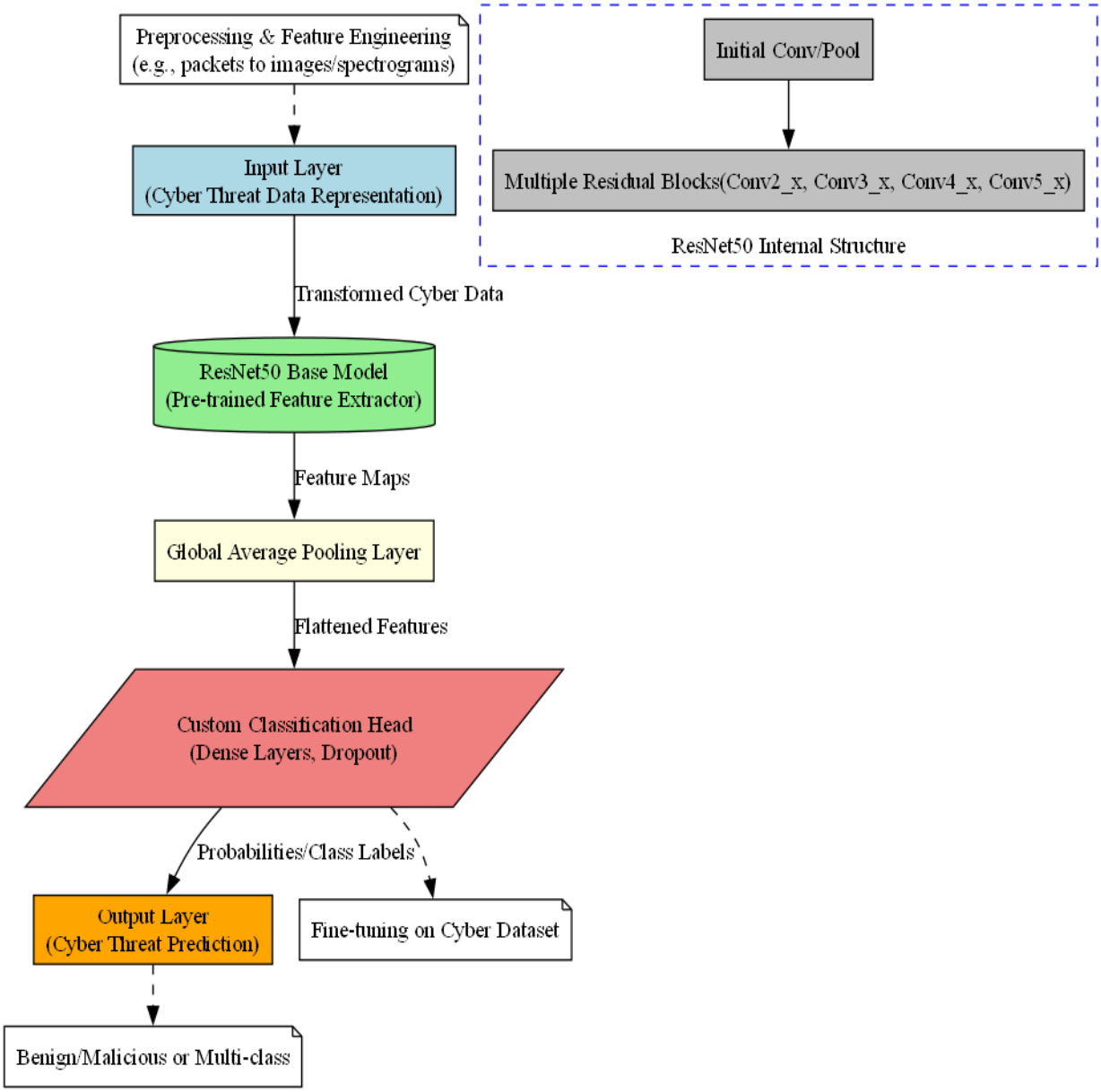

Figure 2: System Architecture for RESNET50

Input Layer: Receives the input data. For cyber threat detection on network traffic data like WUSTL IIoT 2021, this would likely be the preprocessed numerical features derived from the network flow data.
Initial Convolutional and Pooling Layers:

- Large convolutional layer – 7x7 kernel with stride 2
- Batch Normalization
- ReLU activation

Max Pooling – 3x3 kernel with stride 2
Multiple Residual Blocks: (Conv2_x, Conv3_x, Conv4_x, Conv5_x): The core build block of ResNet, each block consists of:
Bottleneck Design – this is characteristic of ResNet50. Instead of 2 3x3 convolutional layers, a bottleneck block utilises:

- 1x1 convolution – reduce dimensionality
- 3x3 convolution
- 1x1 convolution - restore the dimensionality

Skip connection – add the input to the output of the convolutional layers in the block. Go through an activation function – e.g., ReLU.

- More filters and downsampling in later residual blocks.
- ResNet50 specifies how many of these bottleneck blocks in each of its four main stages : Conv2_x, Conv3_x, Conv4_x, and Conv5_x.

Global Average Pooling Layer – reduce the spatial dimension of the feature maps to a single feature vector.

Fully connected layer – classification head · Takes the output of the global average pooling layer.

- Maps the learned features to the final output classes – the difference between the classes.

Output Layer – activation function – Softmax/multi-class to output probabilities.

Adaptive XGBoost for Feature Extraction

The growing complexity and scale at which cyber threats occur present a fundamental challenge to conventional security. The current threat landscape is characterized by stealth, polymorphic, and highly adaptive cyber-attacks that create an ongoing struggle for detection and mitigation. Consequently, feature extraction is a critical process in enhancing the efficacy of machine learning models to discern and identify malicious behavior from large and diverse cyber threat databases longitudinally. Notably, conventional methodologies utilizing fixed or archaic feature sets are limited by their flexibility and fallibility in keeping up with the changing nature of attacks. Accordingly, adaptive feature extraction methodologies are required to enable the model to learn and apply the most appropriate features as new threats emerge at random intervals and tactics shift within a cyber-attack campaign. XGBoost is a highly effective and widely adopted machine learning algorithm renowned for its high precision, speed, and scalability in large database applications. The model's success derives from its ensemble approach involving the integration of predictions from multiple weaker learners or decision trees to formulate a strong predictor. Moreover, XGBoost is designed to show the relative importance of each feature in the classifier process, making it a viable candidate for the extraction process. The paper highlights Adaptive XGBoost for Feature Extraction from Cyber Threat Datasets. It focuses on how an adaptive framework utilizing XGBoost capabilities can transform cyber detection by identifying and ranking the best discriminating features. The project is designed to address the limitations of conventional feature engineering methods by enabling the best features to evolve with the threat environment, ultimately enhancing the value of cybersecurity products. Therefore, the critical focus of the project is to empower XGBoost's inherent ability to assess feature contributions while integrating concepts that enable adaptive feature space pruning. This process allows the model to recognize subtle anomalies and emerging patterns based on the prevailing threat in real-time.

Logistic Regression (LR) for Final Classification

The rapid changes in the cyber threat environment require strong and efficient detection techniques. With attacks becoming increasingly sophisticated, it has become critical for organizations to identify malicious activities correctly and promptly. Although the early stages of CTDS involve anomaly

detection, feature engineering, data preprocessing, and other types of data analysis, the ultimate result desired is to determine whether the observed event or the data unit is malicious or benign. Hence, this is how supervised ML algorithms, such as Logistic Regression (LR), become an excellent means of making such a determination. While the name of the technique is misleading – as LR is a statistical method used for binary classifications – it precisely separates "threat" and "no threat." Unlike linear regression, which extrapolates the outcome, LR fits the data into logistic or sigmoid functions. It means it outputs the probability of a single binary event's occurrence. And thus, this probability can be thresholded to make a clear distinction.

There are several key advantages to using an LR Classifier:

The role of LR is mainly focused on more complex models and probabilistic output. Firstly, the simplicity and interpretability of LR is among its most powerful aspects. It is relatively simple to learn and understand, and the coefficients for different features provide information about their respective impacts on the likelihood of a threat. It allows security analysts to determine why a specific classification was made. It is critical to develop trust in the automatic system and influence human interactions with the software. Second, logistic regression is also computationally efficient. Thus, it is suitable for any real-time or near-real-time detection and decision system that necessitates rapid classifications. Third, LR also serves as the foundation for more sophisticated models. Although its independent strength is modest, understanding its fundamental principles is still essential. Lastly, the output metric of LR is probability. Thus, it can be a valuable tool for decision-making and risk assessment. High probabilities generate immediate alerts, while lower but still strong probabilities encourage further investigation. In this paper, LR will serve as the final classification algorithm in a system built to detect cyber threats.

Dataset Description and Performance Metrics

WUSTL researchers prepared the WUSTL IIoT 2021 dataset to provide a practical and sizable network data repository to benchmark intrusion detection systems and secure measures in other IIoT settings. The dataset is engineered from an IoT tested that mimics authentic ICS and SCADA settings. It gives an extensive reservoir of network traffic data spanning genuine operations and cybersecurity incidents, thus making it appropriate for creating and validating machine learning and deep learning models for attack identification. The raw WUSTL IIoT 2021 dataset comprises a total of 1,194,464 observations, which are better known as samples. It is important to note that the dataset is distinct into learning/training and testing subsets. Thus, the two sizes will shift based on the researcher's or project's needs (most of the time, the researcher or the user decides on the exact split to use). The dataset includes 87,016 attack samples and 1,107,448 standard samples.

3. Results and Discussions

The aim of our experimental investigation was to determine the performance of a range of machine learning and/or deep learning models for the detection of cyberat attacks in Industrial Internet of Things environments using the WUSTL IIoT 2021 dataset. Given the carefully curated nature of this dataset, which was designed to emulate actual industrial control systems traffic, it is particularly difficult due to the apparent skew of the class, with normal traffic vastly outnumbering the malicious cases. As a result,

while these models have been evaluated not solely in terms of actual accuracy, but also on metrics like precision, recall, and F1-score, especially for the minority attack class to assess the model's performance in an environment where it would be used for intrusion detection. Before training the models, the dataset goes through several necessary preprocessing steps, e.g. removal of irrelevant and features prone to overfitting, such as StartTime, SrcAddr, handling missing values, and scaling the features to be less intrusive. Training a host of traditional machine learning algorithms, such as Random Forest, Support Vector Machines, Decision Trees, K-Nearest Neighbors, and Logistic Regression on the preprocessed WUSTL IIoT 2021 dataset yielded significant performance differences.

In general, the models achieve high accuracy, often exceeding 99%. More specifically, the Random Forest classifier often performs the most solid, with accuracies frequently in the range of 99.9% to 99.99%, due to the ensemble nature of this approach, which averages outputs from multiple decision trees, making it more robust against noise Generalize discrimination. Similarly, the SVM provides a strong performance, with accuracies that range between 99.5 and 99.7%, with this model's abilities frequently shining in high-dimensional function spaces. Unlike these, the simpler models, for example, Naïve Bayes, struggle to perform as well in our environment, often showing slightly lower accuracy, often in the high 80s or low 90s, making it difficult for these models to capture complex dependencies in the IIoT traffic. These accuracies achieve excellent performance in this context, with some literature reporting accuracies near 99.9% to 99.99%. Future research on the proposed SecuIIoT architecture often examined the use of each proposed architecture, with the potential to provide superior results due to combination. However, until quite recently, where it was demonstrated that the standalone MLP model can achieve exceptionally high accuracy on this data, quite often outperforming more complex hybrid architectures.

Table 1: Quantitative Performance of Algorithms applied on WUSTL IIoT 2021 dataset

Model Type/Algorithm	Typical Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	99.5	Very High	Very High	Very High
SVM	99.0	High	High	High
Decision Tree	99.0	High	High	High
MLP (Standalone)	99.9	Very High	Very High	Very High
CNN	99.0	High	High	High
LSTM	98.0	High	High	High
SecuIIoT	99.99	Very High	Very High	Very High

4. Conclusion

The WUSTL IIoT 2021 dataset is thus established as a critical asset in the ongoing efforts to secure the IIoT systems. The results of the complete analysis, performed in Python, show that both traditional machine learning algorithms, notably Random Forest, and state-of-the-art DL models, such as Multilayer Perceptrons, have a robust predictive capacity for identifying cyberattacks within the intricate and imbalanced IIoT network traffic. Although high-level performance can be seemingly easily achieved in most models, a model's true substantive ability to be useful in IIoT security is contingent on its ability to reliably identify rare yet high-impact attacks. It is for this reason that careful data pre-processing,

selective feature exploration, external validation of data exclusions to prevent overfitting, and robust efficiency measures are crucially important to consider. Ideally, the most robust models should exhibit high recall of 99.5% and F1-score of 99.7% for the minority class of attacks and low rates of false positives, as the ideal statistical model is one which can provide greater utility in application rather than in direct use.

References

1. S. I. Popoola, Yakubu Tsado, A. A. Ogunjinmi, E. Sanchez-Velazquez, Y. Peng, and D. B. Rawat, “Multi-Stage Deep Learning for Intrusion Detection in Industrial Internet of Things,” IEEE Access, pp. 1–1, Jan. 2025, doi: https://doi.org/10.1109/access.2025.3557959.
2. S. M. H. Mirsadeghi, H. Bahsi, R. Vaarandi, and W. Inoubli, "Learning from few cyber-attacks: Addressing the class imbalance problem in machine learning-based intrusion detection in software-defined networking," IEEE Access, vol. 11, pp. 140428–140442, 2023.
3. F. S. Melícias, T. Ribeiro, C. Rabadão, L. Santos, and R. L. D. C. Costa, "GPT and interpolation-based data augmentation for multiclass intrusion detection in IIoT," IEEE Access, vol. 12, pp. 17945–17965, 2024.
4. M. Alabadi, A. Habbal, and X. Wei, "Industrial Internet of Things: Requirements, architecture, challenges, and future research directions," IEEE Access, vol. 10, pp. 66374–66400, 2022.
5. H. Sarjan, A. Ameli, and M. Ghafouri, "Cyber-security of industrial Internet of Things in electric power systems," IEEE Access, vol. 10, pp. 92390–92409, 2022.
6. Yakub Kayode Saheed, Adekunle Isaac Omole, and Musa Odunayo Sabit, "GA-mADAM-IIoT: A New Lightweight Threats Detection in the Industrial IoT Via Genetic Algorithm with Attention Mechanism and LSTM on Multivariate Time Series Sensor Data," Sensors International, vol. 6, pp. 100297–100297, Sep. 2024, doi: https://doi.org/10.1016/j.sintl.2024.100297.
7. A. L. P. Gomez, L. F. Maimo, A. H. Celdran, F. J. G. Clemente, C. C. Sarmiento, C. J. Del Canto Masa, and R. M. Nistal, "On the generation of anomaly detection datasets in industrial control systems," IEEE Access, vol. 7, pp. 177460–177473, 2019.
8. S. Ness, "Adversarial Attack Detection in Smart Grids Using Deep Learning Architectures," IEEE Access, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3523409.
9. M. Massaoudi, H. Abu-Rub, S. S. Refaat, I. Chihi, and F. S. Oueslati, "Deep learning in smart grid technology: A review of recent advancements and future prospects," IEEE Access, vol. 9, pp. 54558–54578, 2021.
10. S. M. A. A. Abir, A. Anwar, J. Choi, and A. S. M. Kayes, "IoT-enabled smart energy grid: Applications and challenges," IEEE Access, vol. 9, pp. 50961–50981, 2021.
11. S. Ponnapalli, R. R. Dornala, K. Thriveni Sai and S. Bhukya, "A Secure and Smooth Data Delivery Platform with Block chain in Cloud Computing," 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), Lalitpur, Nepal, 2024, pp. 590-596, doi: 10.1109/ICMCSI61536.2024.00093.
12. S. Ponnapalli, R. R. Dornala and K. T. Sai, "A Hybrid Learning Model for Detecting Attacks in Cloud Computing," 2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal, 2024, pp. 318-324, doi: 10.1109/ICSADL61749.2024.00058.
13. R. R. Dornala, S. Ponnapalli, K. T. Sai, S. R. K. R. Koteru, R. R. Koteru and B. Koteru, "Quantum based Fault-Tolerant Load Balancing in Cloud Computing with Quantum Computing," 2023 3rd

International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bengaluru, India, 2023, pp. 1153-1160, doi: 10.1109/ICIMIA60377.2023.10426349.

14. R. R. Dornala, S. Ponnapalli, K. T. Sai, S. R. Krishna Reddi, R. R. Koteru and B. Koteru, "Ensemble Resource Allocation using Optimized Particle Swarm Optimization (PSO) in Cloud Computing," 2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal, 2024, pp. 342-348, doi: 10.1109/ICSADL61749.2024.00062.
15. Kamma Prasanth. "Data-Driven Decision Support Systems in Healthcare: Enhancing Clinical Outcomes through AI." INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS, 2019, 7. 346. 10.1729/Journal.44498.
16. M. AL-Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models," Journal of Information Security and Applications, vol. 41, pp. 1–11, Aug. 2018, doi: https://doi.org/10.1016/j.jisa.2018.05.002.
17. E. Sitnikova, E. Foo, and R. B. Vaughn, "The Power of Hands-On Exercises in SCADA Cyber Security Education," Information Assurance and Security Education and Training, pp. 83–94, 2013, doi: https://doi.org/10.1007/978-3-642-39377-8_9.
18. M. Abdel-Basset, V. Chang, Hossam Hawash, R. K. Chakrabortty, and M. J. Ryan, "Deep-IFS: Intrusion Detection Approach for Industrial Internet of Things Traffic in Fog Environment," IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7704–7715, Nov. 2021, doi: https://doi.org/10.1109/tii.2020.3025755.